

**Teoría de las Comunicaciones**  
12 de Diciembre de 2018  
2<sup>do</sup> Recuperatorio



Departamento de Computación  
Facultad de Ciencias Exactas y Naturales  
Universidad de Buenos Aires

Apellido: _____	Orden: _____	Hojas >	Ej.1	Ej.2	Ej.3	Ej.4	TOT
Nombres: _____	LU: _____	Calif. >	2	1	1	2	6
			B	B	B	R	Final: (A)

Todas las respuestas se consideran válidas solo si están debidamente justificadas.  
Entregar cada ejercicio en hojas separadas.

### Ejercicio 1

Un dispositivo que conecta dos hosts (A y B), inspecciona los paquetes que se envían entre ellos, pero tiene problemas de conectividad y obtiene la siguiente traza incompleta:

#	ORIG	DEST	FLAGS	#SEQ	#ACK	LENGTH
	A:5000	B:6000	S	0	—	
	A:5000	B:6000	A	1	1001	
	A:5000	B:6000		1	1001	150
	A:5000	B:6000		151	1101	150
	B:6000	A:5000	A	1101	301	50
	A:5000	B:6000	F	301	1251	

- Completar la traza sabiendo que A envía 300 bytes, B responde 150 bytes, y luego ambos pasan por el estado CLOSING.
- Ahora suponiendo que cada dos paquetes con datos, la red descartara uno. ¿Cómo modificaría la traza para que exponga ese comportamiento? *Nota: Se puede reescribir la traza o solo detallar y justificar los cambios.*

### Ejercicio 2

Un usuario con casilla de correo en undominio.org.ar envía un mail desde su user agent a otro usuario con casilla en el dominio otrodominio.org.ar.

- Describe las conexiones TCP se establecen desde que lo envía un usuario hasta que el otro lo recibe, mencionando a qué protocolos de capa de aplicación están relacionadas.
- Más tarde, el usuario en otrodominio.org.ar, abre en su PC un Navegador Web para acceder a su casilla vía webmail al sitio webmail.otrodominio.org.ar. Describe la secuencia de mensajes de capa de aplicación que se desencadenan para que el usuario realice un login y visualice su bandeja de entrada.

*Asumir:*

- Los datos del proceso de login se envían mediante un mensaje POST.
- El tamaño de la bandeja de entrada del usuario es lo suficientemente chico como para ocupar sólo un Response HTTP.

### Ejercicio 3

Una conexión recién establecida tiene un RTT=100ms y debe transmitir 70KB. Al principio, el receptor anuncia una *Advertised Window* de 64KB y se sabe que el proveedor de servicio del host emisor limita la velocidad descartando todos los segmentos de una ráfaga si se envían 32KB o más por RTT.

- ¿Cuántos datos lleva transmitidos con éxito (i.e.: datos que ya no están "en vuelo") a los 550ms?
- Si a partir de los 700ms de iniciada la transferencia, los ACKs que arriban al emisor tienen una *Advertised Window* de 16KB ¿Cuanto vale la CWND una vez finalizada la transferencia?

#### Ejercicio 4

Una organización nos pide que implementemos una política de seguridad para su red que tiene las siguientes características:

- 25 hosts de los empleados con información crucial de la compañía.
  - 1 servidor de correo entrante y saliente.
  - 1 servidor DNS que se encarga de resolver todas las operaciones de DNS de la red interna.
  - 1 servidor Proxy para que los usuarios puedan acceder a la web por HTTP y HTTPS.
- a. Presente un esquema gráfico de la red y detalle todas las reglas de firewall necesarias para implementar la política de seguridad especificada.
- b. Los usuarios necesitan poder confiar en que establecen las conexiones con el Proxy verdadero. Explique cómo hacer para garantizar la autenticidad del Proxy del lado de los usuarios, aclarando dónde se instalarían los certificados digitales.



1) a) Brupde 250

#	ORIG	DEST	FLAGS	#seq	#ack	length
1	A	B	S	0	-	
2	B	A	SA	1000	1	
3	A	B	A	1	1001	
4	A	B		1	1001	150
5	B	A	A	1001	151	
6	B	A		1001	151	100
7	A	B	A	151	1101	
8	A	B		151	1101	150
9	B	A	A	1101	301	50
<del>10</del>	<del>B</del>	<del>A</del>				
10	<del>A</del>	<del>B</del>	A	301	1151	
11	B	A		1151	301	100
12	A	B	A	301	1251	
13	A	B	F	301	1251	
14	B	A	F	1251	301	
15	B	<del>A</del>	A	1252	302	
16	<del>A</del>	<del>B</del>	A	302	1252	

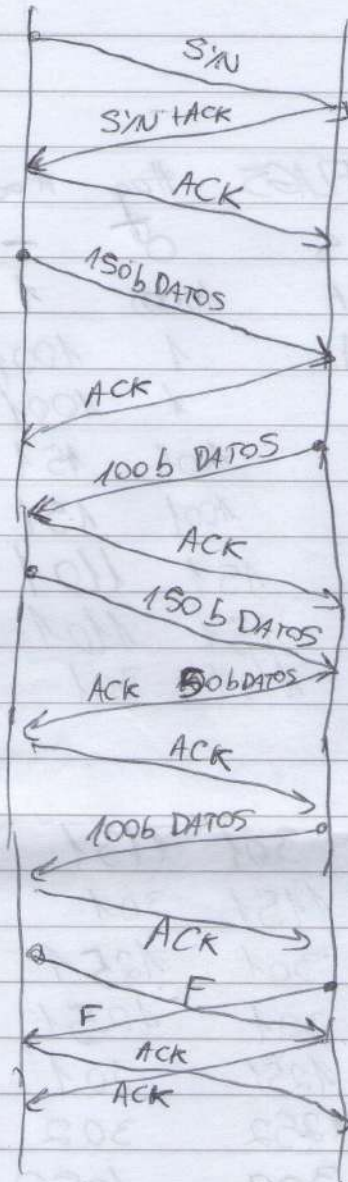
En 15 B está en delay porque recibió el FIN de A

En 16 A está en delay porque " " " " B

En ambos casos se responde un ACK

A

B





D) b) paquetes con datos enviados

en 4 de A a B 150 b

en 6 de B a A 100 b

en 8 de A a B 150 b

en 9 de B a A 50 b

en 11 de B a A 100 b

En este caso se descartarían primero el ~~primer~~ paquete de 100 b que envía B hacia A con lo cual nunca llegarán los ACK de respuesta ✓

Se espera un RTO para reenviar el paquete si no llega la ACK, con lo cual antes de que suceda eso

A le envía a B un paquete de 150 b en 8 que B recibe y notifica con ACK ✓

~~Al respecto de ACKs~~

Luego B reenvía el paquete de 6 pero nuevamente al cae y no llega con lo que al pasar un RTO le vuelve a reenviar momento en el que A lo recibe y responde con ACK ✓

Ahora falta que B envíe 9 y 11 y en ambos casos sucederá que al mandar por primera vez el paquete, este ~~no~~ no llegará con lo que luego de un RTO será retransmitido exitosamente respondiendo con la ACK ✓



B<sup>1</sup>  
2)a)

Cliente

Cliente → Serv SMTP fuente → Serv SMTP destino

El usuario se conecta utilizando el protocolo SMTP a su servidor mail ~~mandándole~~ el mensaje y ~~el correo~~ correo destino. El servidor mail se encuentra en ~~el dominio~~ ~~org.ar~~ ~~org.ar~~.

Luego el servidor mail se ~~conectará~~ ~~conectará~~ a otro, y ~~entonces~~ ~~entonces~~ a otro y así hasta llegar al servidor mail de otro dominio. Org.ar  
Vía SMTP enviando el correo destino y el mensaje.

Finalmente el usuario destino ~~descargará~~ ~~descargará~~ los mails a su PC utilizando el protocolo POP3 o IMAP, habiendo ~~conectado~~ ~~conectado~~.

Finalmente el usuario se conectará a su servidor mail y descargará los correos para poder visualizarlos ~~utilizando~~ ~~utilizando~~ POP3 o IMAP.

Todo esto fue realizado sobre TCP, la consulta DNS sobre UDP.

b) Primero se conecta ~~via~~ ~~via~~ ~~via~~ al sitio necesita visualizar la página.

GET /index.html HTTP 1.1

Host: webmail.stodominio.org.ar

RESPONSE 200 OK  
data

Asume que la página no utiliza recursos de ningún otro  
y que el cuerpo no recibe

POST: user forward HTTP/1.1  
Host: web-mail.stadmanis.org.ar

RESPONSE 200 OK  
data

Envío la data y se me responde con la bandeja de  
entrada para poder ver vinculos

Falta  
DWS.



3) RTT = 100 ms 70 kb

BIEN

AW = 64 kb se descarta en 32 Kb

Todos los números representan KB

last byte sent last rx window

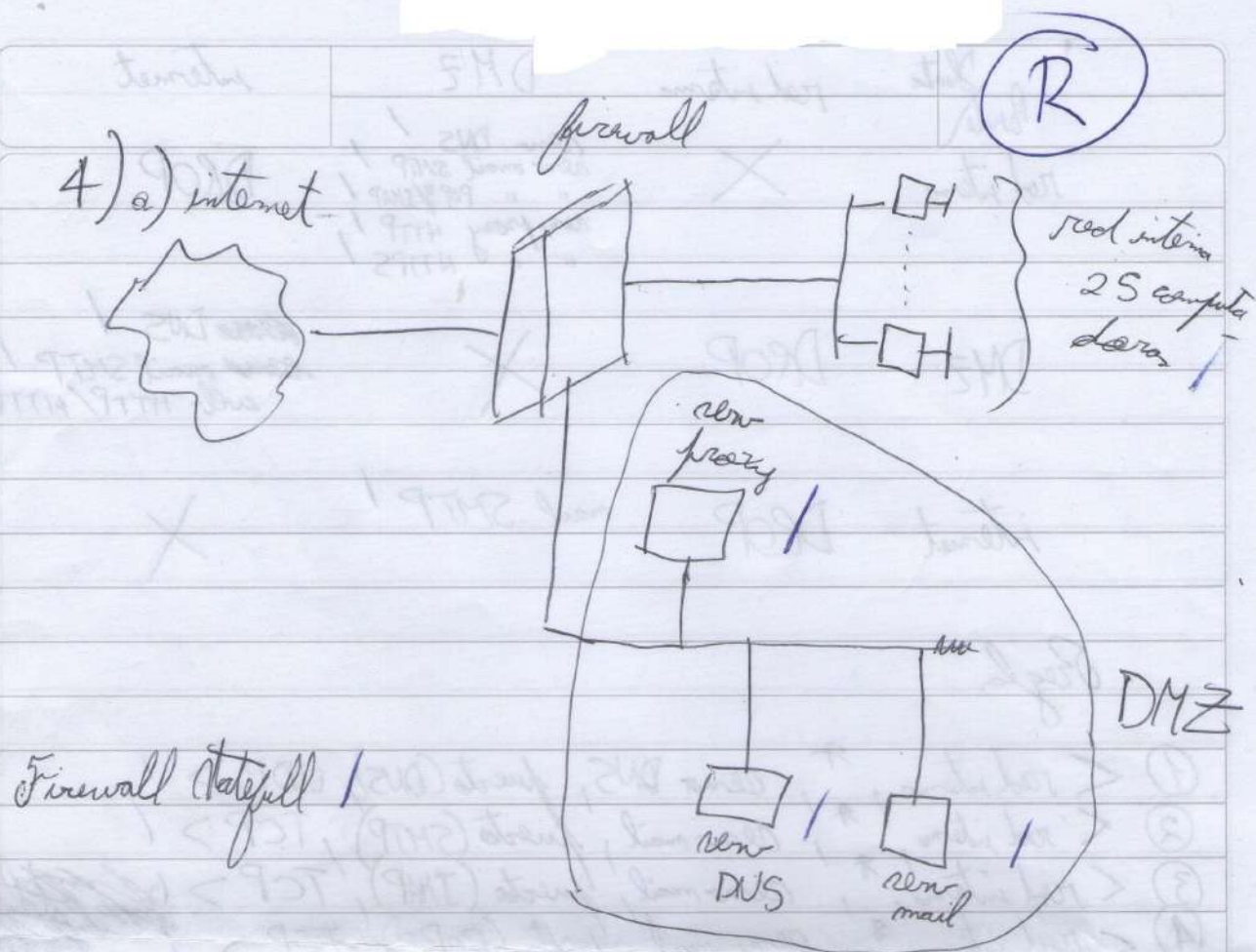
	RTT	CWND	RWND	SSTHRESH	LB	LA	FS
	1	4	64	64	4	0	4
	2	8	64	64	12	4	8
	3	16	64	64	28	12	16
	4	32	64	64	60	28	32
aca se descarta	5	32	64	64	60	28	32 - 500 ms
	6	2	64	16	30	28	2 - 600 ms
como nunca llegan back a preceder	7	4	<del>64</del> 16	16	34	30	4 - 700 ms
hay un RTO	8	8	<del>16</del> 16	16	42	34	8
	9	16	<del>16</del> 16	16	58	42	16
hay un timer out	10	18	<del>16</del> 16	16	70	58	<del>16</del> 12
	11	20	<del>16</del> 16	16			

para congestion avoidance

$$\begin{aligned}
 \text{SSTHRESH luego del time out} &= \max(FS/2, 2^8 SFS) \\
 &= \max(32/2, 2^8 2) \\
 &= \max(16, 4) \\
 &= 16
 \end{aligned}$$

- a) Entramento al transmisor en 20 Kb ✓  
 b) 20 Kb



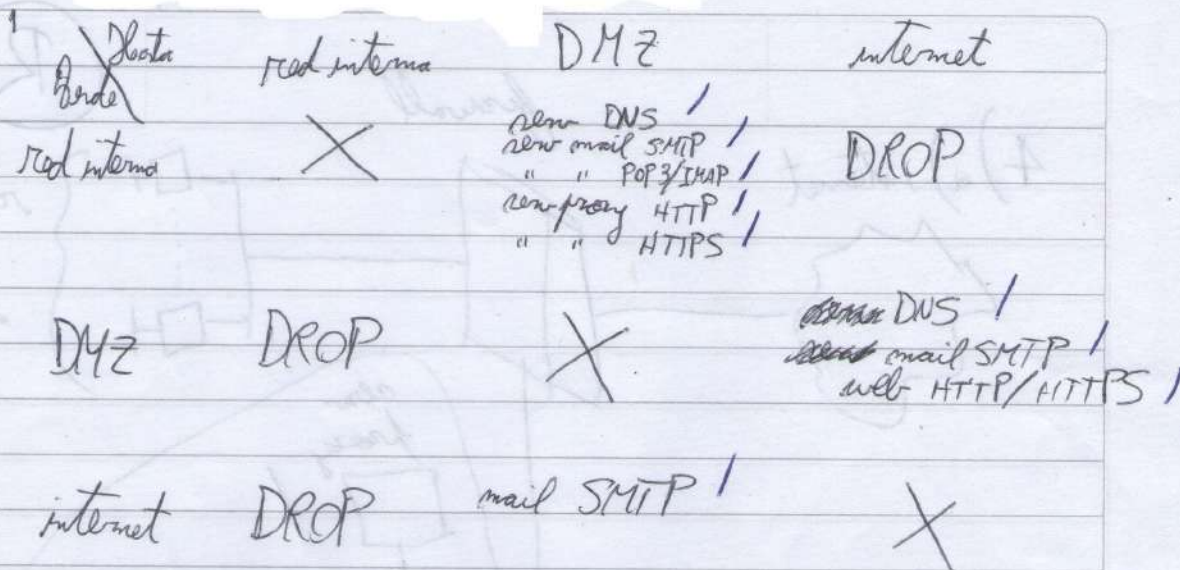


Los usuarios de la red interna deberían poder tener acceso al proxy, al servidor de mail y al DNS para resolver las consultas sobre los otros dos servidores.

Desde la DMZ solo se puede acceder a internet para consulta, HTTP, HTTPS, consulta de DNS, SMTP.

Desde internet solo se puede acceder al servidor mail.

~~El firewall es un dispositivo que protege la red interna de ataques externos.~~



### Reglas

- ① < red interna, \*, allow DNS, puerto(DNS), UDP > /
- ② < red interna, \*, allow mail, puerto(SMTP), TCP > /
- ③ < red interna, \*, allow mail, puerto(IMAP), TCP > /
- ④ < red interna, \*, allow mail, puerto(POP3), TCP > /
- ⑤ < red interna, \*, allow proxy, puerto(HTTP) (80), TCP > /
- ⑥ < red interna, \*, allow proxy, puerto(HTTPS), TCP > /
- ⑦ < allow proxy, \*, internet, puerto(DNS), UDP > /
- ⑧ < allow proxy, \*, internet, puerto(HTTP), TCP > /
- ⑨ < allow proxy, \*, internet, puerto(HTTPS), TCP > /
- ⑩ < allow mail, \*, internet, puerto(SMTP), TCP > /
- ⑪ < internet, \*, allow mail, puerto(SMTP), TCP > /



4)b) Implementa un sistema de clave simétrica donde los usuarios tienen clave <sup>pública</sup> privada y el proxy clave <sup>pública</sup> privada. Al querer conectar con el proxy se envían un challenge response con un valor encriptado por

4)b) Implementa un sistema de clave simétrica con 1 clave pública y 2 privadas, el usuario encripta y envía un challenge response encriptado con la clave privada que el proxy debe desencriptar y responder.

No usas certificados (X)

No validas Al proxy con ese challenge/response  
Sino al usuario (X)